リモート リーフ スイッチ

この章で説明する内容は、次のとおりです：

ACI ファブリックのリモート リーフ スイッチについて

ACI ファブリックの展開では、ローカルスパインスイッチまたは APIC が接続されていない Cisco ACI リーフスイッチのリモートデータセンタに、ACI サービスと APIC 管理を拡張できます。

リモート リーフ スイッチがファブリックの既存のポッドに追加されます。メインデータセンターに展開されるすべてのポリシーはリモートスイッチで展開され、ポッドに属するローカルリーフスイッチのように動作します。このトポロジでは、すべてのユニキャストトラフィックはレイヤ 3 上の VXLAN を経由します。レイヤ 2 ブロードキャスト、不明なユニキャスト、マルチキャスト（BUM）メッセージは、WAN を使用するレイヤ 3 マルチキャスト（bidirectional PIM）を使用することなく、 Head End Replication（HER）トンネルを使用して送信されます。スパイン スイッチ プロキシを使用する必要があるすべてのトラフィックは、メイン データセンターに転送されます。

APIC システムは、起動時にリモート リーフ スイッチを検出します。その時点から、ファブリックの一部として APIC で管理できます。

（注）
- すべての inter-VRF トラフィック（リリース 4.0(1) 以前）は、転送される前にスパイン スイッチに移動します。
- リリース 4.1(2) 以前では、リモート リーフを解除する前に、vPC を最初に削除する必要があります。

リリース 4.0(1) でのリモート リーフ スイッチの動作の特性

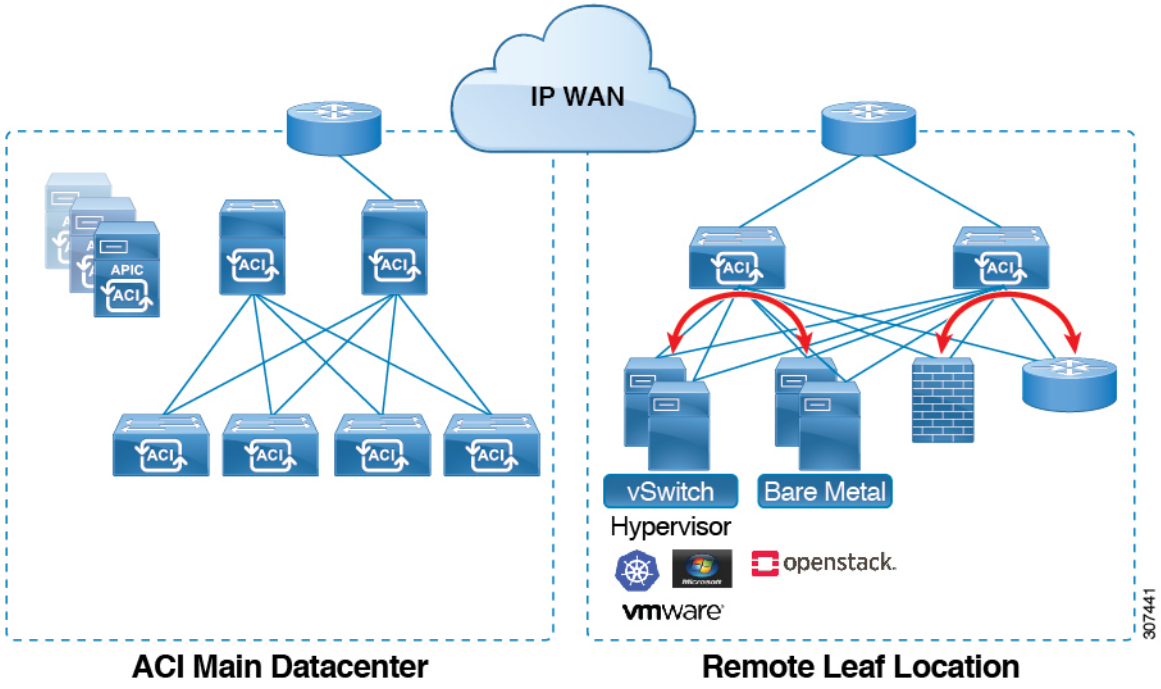
リリース 4.0(1) 以降、リモート リーフ スイッチの動作には次の特徴があります。

- spine-proxy からサービスを切り離すことによって WAN 帯域幅の使用量を削減します。
  - PBR：ローカル PBR デバイスまたは vPC の背後にある PBR デバイスでは、ローカル スイッチングはスパイン プロキシに移動せずに使用されます。ピア リモート リーフ上の孤立ポートの PBR デバイスでは、RL-vPC トンネルを使用します。これは、主要 DC へのスパイン リンクが機能しているか否かを問わず該当します。
  - ERSPAN：ピア接続先 EPG では、RL-vPC トンネルが使用されます。ローカルな孤立ポートまたは vPC ポート上の EPG は、宛先 EPG へのローカル スイッチングを使用します。これは、主要 DC へのスパイン リンクが機能しているか否かを問わず該当します。
  - 共有サービス：パケットはスパイン プロキシ パスを使用しないため WAN 帯域幅の使用量を削減します。
  - Inter-VRF トラフィックは上流に位置するルータ経由で転送され、スパインには配置されません。
  - この機能強化は、リモート リーフ vPC ペアにのみ適用されます。リモート リーフ ペアを介した通信では、スパイン プロキシは引き続き使用されます。
- spine-proxy に到達不能な場合のリモート リーフ ロケーション内の（ToR グリーニング プロセスを通じた）不明な L3 エンドポイントの解像度。

リリース4.1(2) でのリモート リーフ スイッチ動作の特性

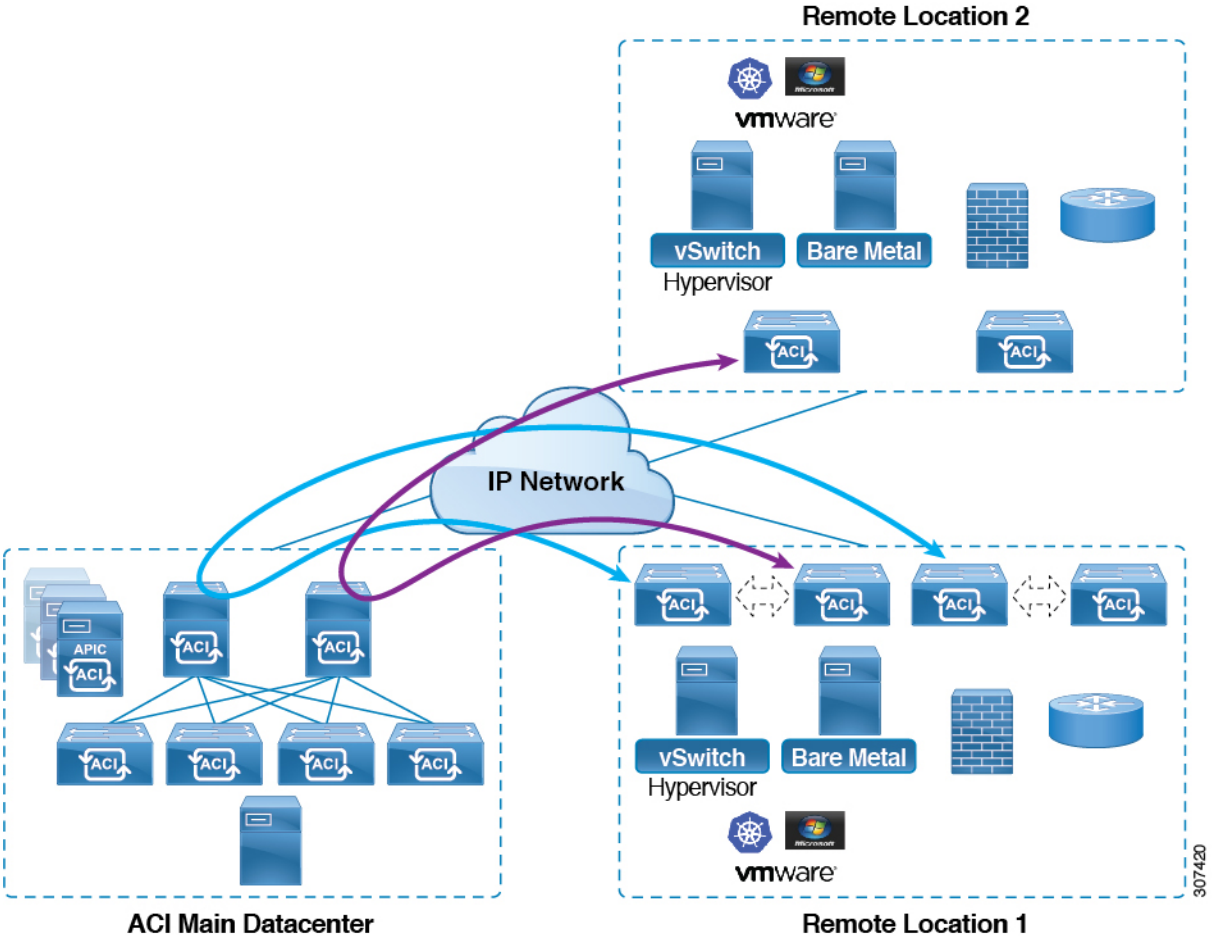
リリース4.1(2) よりも前のリリースでは、次の図に示すように、リモートリーフロケーション上のすべてのローカル スイッチング（リモート リーフ vPC ピア内）トラフィックは、物理的または仮想的にエンドポイント間で直接スイッチングされます。

図 *1 : Local Switching Traffic* : リリース *4.1(2)* 以前



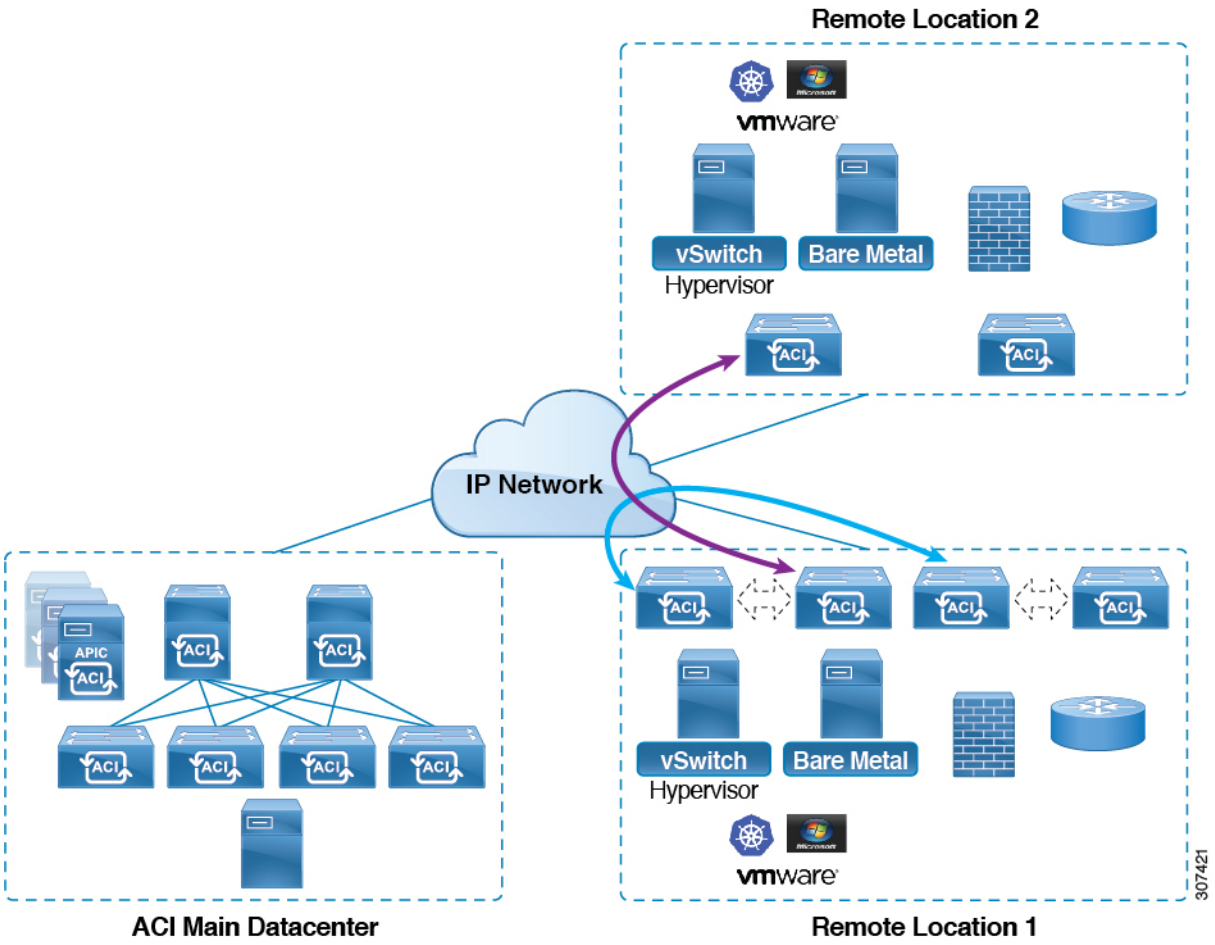
さらに、リリース4.1(2)よりも前では、次の図に示すように、リモートロケーション内またはリモート ロケーション間のリモート リーフ スイッチ vPC ペア間のトラフィックは、ACI メイン データ センター ポッドのスパイン スイッチに転送されます。

図 *2 : Remote Switching Traffic* : リリース *4.1(2)* より以前



リリース 4.1(2) 以降では、異なるリモート ロケーションにあるリモート リーフ スイッチ間の直接トラフィック転送がサポートされるようになりました。この機能は、次の図に示すように、リモート ロケーション間の接続に一定レベルの冗長性と可用性を提供します。

図 *3 : Remote Leaf Switch Behavior* : リリース *4.1(2)*



また、リリース 4.1(2) 以降でも、リモート リーフ スイッチの動作には次の特徴があります。

- リリース 4.1(2) 以降、ダイレクト トラフィック転送では、シングル ポッド設定内でスパイン スイッチに障害が発生すると、次のようになります。
  - ローカル スイッチングは、上記の「ローカル スイッチング トラフィック：リリース 4.1(2) 以前」に示すように、リモート リーフ スイッチ vPC ピア間の既存および新規のエンドポイント トラフィックに対して機能し続けます。
  - リモート ロケーション間のリモート リーフ スイッチ間のトラフィックの場合：
    - リモート リーフ スイッチからスパイン スイッチへのトンネルがダウンするため、新しいエンドポイント トラフィックは失敗します。リモート リーフ スイッチから、新しいエンドポイントの詳細はスパイン スイッチに同期されないため、同じまたは異なる場所にある他のリモート リーフ スイッチ ペアは、COOP から新しいエンドポイント情報をダウンロードできません。
    - 単方向トラフィックの場合、既存のリモートエンドポイントは300秒後にエージングアウトするため、そのポイント以降のトラフィックは失敗します。ポッド内

のリモート リーフ サイト内（リモート リーフ VPC ペア間）の双方向トラフィックは更新され、引き続き機能します。リモート ロケーション（リモート リーフ スイッチ）への双方向トラフィックは、900 秒のタイムアウト後に COOP によってリモートエンドポイントが期限切れになるため、影響を受けることに注意してください。

- 共有サービス（VRF 間）の場合、同じポッド内の 2 つの異なるリモート ロケーションに接続されたリモート リーフ スイッチに属するエンドポイント間の双方向トラフィックは、リモート リーフ スイッチ COOP エンドポイントのエージアウト時間（900秒）後に失敗します。これは、リモートリーフスイッチからスパインへの COOP セッションがこの状況でダウンするためです。ただし、2 つの異なるポッドに接続されたリモート リーフ スイッチに属するエンドポイント間の共有サービス トラフィックは、COOP 高速エージング タイムである 30 秒後に失敗します。
- スパイン スイッチへの BGP セッションがダウンするため、L3Out 間通信は続行できません。

- トラフィックが 1 つのリモート リーフ スイッチから送信され、別のリモート リーフ スイッチ（送信元の vPC ピアではない）に送信されるリモート リーフ直接単方向トラフィックがある場合は、300 秒のリモート エンド ポイント（XR EP）タイムアウトが発生するたびに、ミリ秒単位のトラフィック損失が発生します。
- ACI Multi-Site 設定を使用したリモート リーフ スイッチでは、スパイン スイッチに障害が発生しても、リモート リーフ スイッチから他のポッドおよびリモート ロケーションへのすべてのトラフィックが継続します。これは、この状況ではトラフィックが代替の使用可能なポッドを通過するためです。

リモート リーフ スイッチの IPN での 10 Mbps 帯域幅のサポート

リモート リーフ スイッチからのデータ トラフィックのほとんどがローカルで、ポッド間ネットワーク（IPN）が管理目的でのみ必要な場合があります。このような状況では、100 Mbps の IPN は必要ない場合があります。これらの環境をサポートするために、リリース 4.2(4) 以降、IPN の最小帯域幅として 10 Mbps のサポートが利用可能になりました。

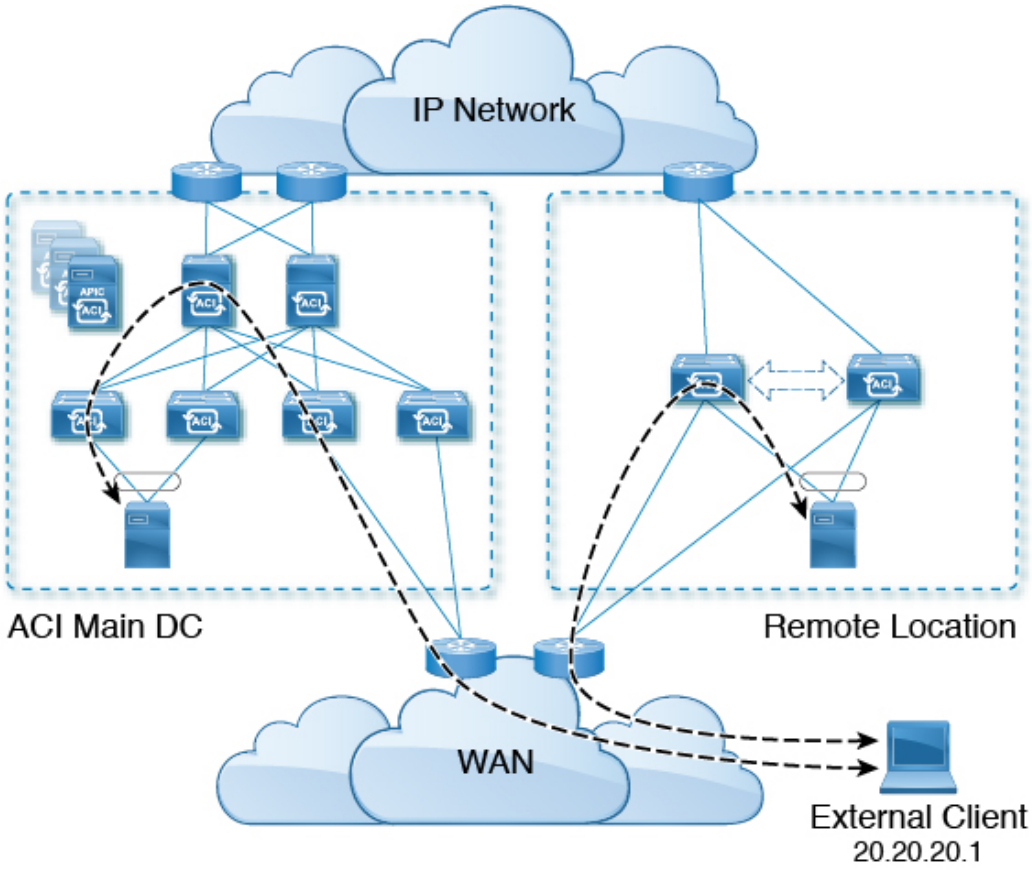
これをサポートするには、次の要件を満たす必要があります。

- IPN パスは、リモート リーフ スイッチ（アップグレードおよびダウングレード、ディスカバリ、COOP、ポリシー プッシュなどの管理機能）の管理にのみ使用されます。
- 「Cisco APIC GUI を使用した DSCP 変換ポリシーの作成」の項に記載されている情報に基づいて、Cisco ACI データセンターとリモート リーフ スイッチ ペア間のコントロールおよび管理プレーン トラフィックに優先順位を付けるために、QoS 構成を使用して IPN を構成します。
- [Cisco ACI] データセンターおよびリモート リーフ スイッチからのすべてのトラフィックは、ローカル L3Out を経由します。

- EPG またはブリッジ ドメインは、リモート リーフ スイッチと ACI メイン データセンター間で拡張されません。
- アップグレード時間を短縮するには、リモート リーフ スイッチにソフトウェア イメージを事前にダウンロードする必要があります。

次の図に、この機能のグラフィカル表示を示します。

図 *4 :* リモート リーフ スイッチ動作（リリース *4.2*（*4*））：*IPN* でのリモート リーフ スイッチの管理

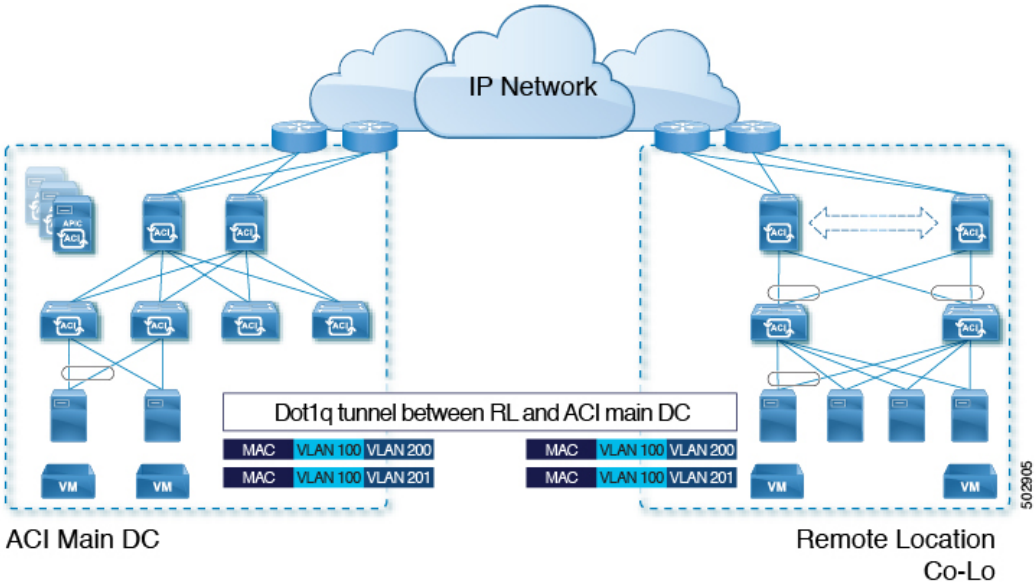


リモート リーフ スイッチでの Dot1q トンネルのサポート

状況によっては、コロケーションプロバイダーが複数のカスタマーをホストしており、各カスタマーがリモート リーフ スイッチ ペアごとに数千の VLAN を使用している場合があります。リリース 4.2(4) 以降では、リモート リーフ スイッチと ACI メイン データセンター間に 802.1Q トンネルを作成するためのサポートを利用できます。これにより、複数の VLAN を単一の 802.1Q トンネルに柔軟にマッピングできるため、EPG の拡張要件が軽減されます。

次の図に、この機能のグラフィカル表示を示します。

図 *5:* リモート リーフ スイッチの動作、リリース *4.2*（*4*）：リモート リーフ スイッチでの *802.1Q* トンネル サポート



[Cisco APIC レイヤ *2* ネットワーク構成ガイド（*Cisco APIC Layer 2 Networking Configuration Guide*）*]*の「802.1Q Tunnels」の章に記載されている手順を使用して、リモート リーフ スイッチと ACI メイン データセンター間にこの 802.1Q トンネルを作成します。これは、[Cisco APIC ドキュメンテーション ランディング ページ（Cisco APIC documentation landing page）]にあります。

ウィザードを使用するか（使用しない場合も）、REST API または NX-OS スタイル CLI を使用して、APIC GUI のリモート リーフ スイッチを構成できます。

リモート リーフ スイッチのハードウェアの要件

リモート リーフ スイッチの機能には、次のスイッチがサポートされています。

ファブリック スパイン スイッチ

WAN ルータに接続される [Cisco アプリケーション セントリック インフラストラクチャ（Cisco Application Centric Infrastructure）]（[ACI]）メイン データ センターでのスパイン スイッチとしては、次のスパイン スイッチがサポートされています。

- 固定スパイン スイッチ Cisco Nexus 9000 シリーズ
  - N9K-C9332C
  - N9K-C9364C
  - すべての GX および GX2 スイッチ
- モジュラー スパイン スイッチとしては、EX 以降で終了する名前の Cisco Nexus 9000 シリーズ スイッチのみがサポートされます（たとえば N9K-X9732C- EX ）。

- 古い世代のスパイン スイッチ、たとえば固定スパイン スイッチ N9K-C9336PQ や、N9K X9736PQ ライン カードを搭載したモジュラー スパイン スイッチなどは、メイン データセンターではサポートされますが、WAN への接続がサポートされるのは次世代のスパイン スイッチのみです。

リモートのリーフ スイッチ

- リモートのリーフ スイッチ、後で (たとえば N9K-C93180LC-EX) EX で終了する名前と Cisco Nexus 9000 シリーズ スイッチのみがサポートされています。
- リモートのリーフ スイッチする必要がありますにイメージを実行する、スイッチ 13.1.x 以降 (aci n9000 dk9.13.1.x.x.bin) 検出できる前にします。これにより、リーフ スイッチでの手動アップグレードが必要があります。

リモート リーフ スイッチの制約事項と制限事項

リモート リーフには、次の注意事項および制約事項が適用されます。

- リモート リーフ ソリューションでは、リモート リーフ スイッチとメイン データ センターのリーフ/スパイン スイッチの /32 トンネル エンド ポイント（TEP）IP アドレスが、要約なしでメイン データ センターとリモート リーフ スイッチ間でアドバタイズされる必要があります。
- リモート リーフ スイッチを同じポッド内の別のサイトに移動し、新しいサイトに元のサイトと同じノード ID がある場合は、仮想ポート チャネル（vPC）を削除して再作成する必要があります。
- Cisco N9K-C9348GC-FXP スイッチでは、ポート 1/53 または 1/54 でのみ最初のリモート リーフ スイッチ ディスカバリを実行できます。その後、リモート リーフ スイッチの ISN/IPN へのファブリック アップリンクに他のポートを使用できます。
- 6.0（3）リリース以降、ダイナミック パケットの優先順位付けが有効になっておりCoS 保存ポリシーまたは [Cisco ACI マルチポッド（Cisco ACI Multi-Pod）] ポリシーが有効になっている場合、予想される動作は、 CoS 保存も有効にしている場合、または [Cisco ACI マルチポッド（Cisco ACI Multi-Pod）] ダイナミックパケット プライオリティ設定と連動する DSCP 変換。ただし、実際の動作は次のとおりです：
  - 物理リーフおよびリモート リーフ スイッチでダイナミック パケットの優先順位付け機能を使用して CoS 保持を有効にした場合、マウス フローは VLAN CoS 優先順位 0 でファブリックを出ます。
  - を有効にすると、マウス フローは VLAN CoS 優先順位 0 でファブリックを出ます。[Cisco ACI マルチポッド（Cisco ACI Multi-Pod）] 物理リーフスイッチでのダイナミック パケット優先順位付け機能を使用した DSCP 変換。

- を有効にすると、マウス フローは VLAN CoS 優先順位 3 でファブリックを出ます。[Cisco ACI マルチポッド（Cisco ACI Multi-Pod）] リモート リーフ スイッチでのダイナミック パケット優先順位付け機能を使用した DSCP 変換。

[Cisco ACI マルチポッド（Cisco ACI Multi-Pod）] DSCP 変換を有効にしていても、マウス フローがリモート リーフ スイッチを出るときに、マウス フローの VLAN CoS プライオリティが 3 にならないようにするには、代わりに CoS 保存機能を使用します。

ここでは、リモート リーフ スイッチでサポートされるものとサポートされないものについて説明します。

- サポートされる機能 （10 ページ）
- サポートされない機能 （11 ページ）
- リリース 5.0（1）の変更点 （13 ページ）
- リリース 5.2（3）での変更点 （13 ページ）

サポートされる機能

Cisco APIC リリース 6.1（1）以降、ファブリック ポート（アップリンク）は、ルーテッド サブインターフェイスとして、ユーザー テナント L3Out と SR-MPLS インフラ L3Out を伴うように構成できるようになりました。

- リモートリーフ ファブリック ポートでは、ルーテッドサブインターフェイスを伴う L3Out のみが許可されます。
- リモート リーフ ファブリック ポートは、ユーザー テナントの L3Out または SR- MPLS インフラ L3Out としてのみ展開できます。
- アプリケーション EPG にリモート リーフ ファブリックポートを展開することはできません。ルーテッド サブインターフェイスを伴う L3Out のみが許可されます。
- ハイブリッド ポートでは、PTP/同期アクセス ポリシーのみがサポートされます。他のアクセス ポリシーはサポートされません。
- ハイブリッド ポートではファブリック SPAN のみがサポートされます。
- NetFlow は、ユーザー テナント L3Out で構成されたファブリックポートではサポートされません。

Cisco APIC リリース 6.0（4）以降では、vPC リモート リーフ スイッチ ペア間での L3Out SVI のストレッチがサポートされています。

Cisco [APIC] リリース 4.2（4）以降、802.1Q（Dot1q）トンネル機能がサポートされています。

Cisco [APIC] リリース 4.1（2）以降、次の機能がサポートされています：

- [ACI] マルチサイトを持つリモート リーフ スイッチ

- 同じリモート データ センター内の 2 つのリモート リーフ vPC ペア間またはデータ センター間でのトラフィック転送（これらのリモート リーフ ペアが同じポッドまたは同じマルチポッド ファブリックの一部であるポッドに関連付けられている場合）
- メインの Cisco [ACI] データ センター ポッドは、2 つのリモート ロケーション（RL `location-1` の L3Out および RL `location-2` 内の L3Out は、プレフィックスをお互いにアドバタイズします）のトランジットであり、リモート ロケーションに渡って L3Out を移行します。

Cisco [APIC] リリース 4.0（1）以降、次の機能がサポートされています：

- Epg の Q-で-Q カプセル化のマッピング
- リモート リーフ スイッチでの PBR トラッキング（システムレベルのグローバル GIPo が有効になっている場合）
- PBR の復元力のあるハッシュ
- Netflow
- MacSec の暗号化
- ウィザードのトラブルシューティング
- アトミック カウンタ

サポートされない機能

このリリースで、サポート対象外の次の機能を除き、ファブリックおよびテナントの完全なポリシーがリモート リーフ スイッチでサポートされています。

- GOLF
- vPod
- フローティング L3Out
- ローカル リーフ スイッチ（ACI 主要データ センター スイッチ）とリモート リーフ スイッチ間の L3out SVI のストレッチ、または 2 つの異なるリモート リーフ スイッチの vPC ペア間のストレッチ
- コピー サービスは、ローカル リーフ スイッチに導入されている場合、および送信元または宛先がリモート リーフ スイッチにある場合はサポートされません。この状況では、ルーティング可能な TEP IP アドレスはローカル リーフ スイッチに割り当てられません。詳細については、「*Cisco APIC* レイヤ *4* ～ レイヤ *7* サービス導入ガイド」の「Configuring コピー Services」の章の「 コピー Services Limitations」の項を参照してください。このガイドは、「APIC ドキュメンテーション ページ」にあります。
- レイヤ 2 (静的 Epg 意外) を除く接続外部
- VzAny 契約とサービスをコピーします。
- リモートのリーフ スイッチの FCoE 接続

- ブリッジ ドメインまたは Epg のカプセル化をフラッディングします。
- Fast Link Failover ポリシーは、リーフ スイッチとスパイン スイッチ間の ACI ファブリック リンク用であり、リモート リーフ接続には適用されません。リモート リーフ接続のコンバージェンスを高速化するために、Cisco [APIC] リリース 5.2（1）で代替方法が導入されています。
- 遠隔地での管理対象のサービス グラフに接続されたデバイス
- トラフィック ストーム制御
- Cloud Sec 暗号化
- ファーストホップ セキュリティ
- レイヤ 3 マルチキャスト リモート リーフ スイッチ上のルーティング
- メンテナンス モード
- TEP 間アトミック カウンタ

Multi-Site アーキテクチャでリモート リーフ スイッチをサイト間 L3Out 機能と統合する場合、次のシナリオはサポートされません。

- 別々のサイトに関連付けられたリモート リーフ スイッチのペアに展開された L3Out 間のトランジット ルーティング
- リモート サイトに関連付けられたリモート リーフ スイッチのペアに展開された L3Out と通信するサイトに関連付けられたリモート リーフ スイッチのペアに接続されたエンドポイント
- リモート サイトに関連付けられたリモート リーフ スイッチのペアに展開された L3Out と通信するローカル サイトに接続されたエンドポイント
- リモート サイトに展開された L3Out と通信するサイトに関連付けられたリモート リーフ スイッチのペアに接続されたエンドポイント

（注） 異なるデータ センター サイトが同じマルチポッド ファブリックの一部としてポッドとして展開されている場合、上記の制限は適用されません。

リモート リーフ スイッチ機能では、次の導入と設定がサポートされていません。

- 特定のサイト（[APIC] ドメイン）と Multi-Site デプロイメント（これらのリーフ ノードがローカルまたはリモートである両方のシナリオで）の別のサイトの一部のリーフ ノードに関連付けられたリモート リーフ ノード間のブリッジ ドメインを拡張することはサポートされていません。この制限を強調するために障害が [APIC] に生成されます。これは、Multi-Site Orchestrator（MSO）でストレッチ ブリッジドメインを構成するときに、BUM フラッディングが有効または無効であることとは無関係です。ただし、ブリッジドメイン

は、同じサイト（[APIC] ドメイン）に属するリモート リーフ ノードとローカル リーフ ノード間で常に拡張できます（BUM フラッディングを有効または無効にします）。

- リモート リーフ スイッチ ロケーションおよび主要データセンター全体でのスパニング ツリー プロトコル
- [APIC] は、リモート リーフ スイッチに直接接続されます。
- vPC ドメインでの、リモート リーフ スイッチ上の孤立ポート チャネルまたは物理ポート（この制限は、リリース 3.1 以降に適用します）。
- コンシューマ、プロバイダー、およびサービス ノードがすべてリモート リーフ スイッチに接続されていて、vPC モードである場合、サービス ノード統合の有無に関わらず、リモート ロケーション内でのローカル トラフィック転送のみサポートされます。
- スパイン スイッチから IPN にアドバタイズされる /32 ループバックは、リモート リーフ スイッチに向けて抑制/集約してはなりません。/32 ループバックは、リモート リーフ スイッチにアドバタイズする必要があります。

リリース 5.0（1）の変更点

Cisco [APIC] リリース 5.0（1）以降では、リモート リーフ スイッチに次の変更が適用されています。

- 直接トラフィック転送機能はデフォルトで有効になっており、ディセーブルにできません。
- リモート リーフ スイッチの直接トラフィック転送を使用しない設定はサポートされなくなりました。リモート リーフ スイッチがあり、Cisco [APIC] リリース 5.0（1）にアップグレードする場合は、「Direct Traffic Forwardingについて」の項に記載されている情報を確認し、その項の手順を使用して直接トラフィック転送を有効にします。

リリース 5.2（3）での変更点

Cisco [APIC] リリース 5.2（3）以降では、リモート リーフ スイッチに次の変更が適用されています：

- リモート リーフ スイッチとアップストリーム ルータ間のピアへの IPN アンダーレイ プロトコルは、OSPF または BGP のいずれかです。以前のリリースでは、OSPF アンダーレイのみがサポートされています。

WAN ルータとリモート リーフ スイッチ設定の注意事項

リモート リーフが検出され APIC 管理に組み込まれる前に、WAN ルータとリモート リーフ スイッチを設定する必要があります。

次の要件に従い、ファブリック スパイン スイッチの外部インターフェイスとリモート リーフ スイッチ ポートに接続する WAN ルータを接続します。

WAN ルータ

- エリアID、タイプ、コストなど、同じ詳細を有するインターフェイスでOSPFを有効にします。
- メインファブリックの各APICのIPアドレスにつながるインターフェイスでDHCPリレーを設定します。
- スパイン スイッチでVLAN 5インターフェイスに接続するWANルータのインターフェイスは、通常のマルチポッドネットワークに接続するインターフェイス以外に、異なるVRFに存在する必要があります。

リモート リーフ スイッチ

- ファブリック ポートの1つから直接接続して、アップストリーム ルータにリモート リーフ スイッチを接続します。アップストリーム ルータへの次の接続がサポートされています。
  - 40 Gbps以上の接続
  - QSFP-SFP アダプタでは、1/10 G SFPがサポートされています

  WANの帯域幅は、リリースによって異なります。
  - 4.2(4) 以前のリリースでは、WANの帯域幅は最小で100 Mbps、サポートされている最大遅延は300ミリ秒です。
  - 4.2(4) 以降のリリースでは、WANの帯域幅は最小で10 Mbps、サポートされている最大遅延は300ミリ秒です。
- 上記が推奨されますが、vPCとリモート リーフ スイッチのペアを接続する必要はありません。vPCの両端にあるスイッチは、同じリモートデータセンタのリモートリーフスイッチである必要があります。
- 一意のIPアドレスを持つVLAN 4でレイヤ3サブインターフェイスとしてノース バウンド インターフェイスを設定します。

  リモートのリーフスイッチからルータに1個以上のインターフェイスを接続する場合、一意のIPアドレスで各インターフェイスを設定します。
- インターフェイスでOSPFをイネーブルにしますが、OSPFエリア タイプをスタブ エリアとして設定しないでください。
- リモート リーフ スイッチ内のTEP プール サブネットのIPアドレスは、ポッドTEPサブネットプールと重複しないようにする必要があります。使用されるサブネットは/24以下である必要があります。
- マルチポッドがサポートされますが、リモート リーフ機能は必要ありません。
- 単一ポッド ファブリックのポッドをリモート リーフ スイッチに接続するとき、スパイン スイッチからWANルータへ、リモート リーフ スイッチからWANルータへL3Outを設定し、これは両方ともスイッチ インターフェイスでVLAN-4を使用します。

- マルチポッド ファブリックのポッドをリモート リーフ スイッチに接続するとき、スパイン スイッチから WAN ルータへ 、リモート リーフ スイッチから WAN ルータへ L3Out を設定し、これは両方ともスイッチ インターフェイスで VLAN-4 を使用します。また、VLAN-5 を使用してマルチポッド内部 L3Out を設定し、リモート リーフ スイッチを宛先としてポッドを通過するトラフィックをサポートします。VLAN 4 および VLAN 5 を使用する限り、通常のマルチポッドおよびマルチポッド内部接続は、同じ物理インターフェイスで設定できます。
- マルチポッド内部 L3Out を構成する場合、通常のマルチポッド L3Out と同じルータ ID を使用します。しかし、router-id の **ループバック アドレスとしてのユーザー ルータ ID** オプションを選択して、別のループバック IP アドレスを構成します。これで ECMP が機能します。
- 6.0(1) リリース以降、リモート リーフ スイッチは、サブネット マスクが最大 /28 のリモート プールをサポートします。以前のリリースでは、リモート リーフ スイッチは、サブネット マスクが最大 /24 のリモート プールをサポートしていました。リモート プールを削除できるのは、使用を停止し、そのプールを使用しているすべてのノードを含むファブリックから削除した後でのみです。

  /28 リモート TEP プールは、2 つの vPC ペアを持つ最大 4 つのリモート リーフ スイッチをサポートします。RMA の目的では、2 つの IP アドレスを未使用のままにしておくことをお勧めします。これらの 2 つの IP アドレスは、1 つのスイッチの RMA を行うのに十分です。次の表は、リモート リーフ スイッチがこれらの IP アドレスをどのように使用するかを示しています。

（注） 2 つの IP アドレスが内部ファブリックの使用に使用されます。

IP アドレスタイプ	数量
/28 プールで使用可能な使用可能な IP アドレスの合計	16 - 2 = 14
ファブリックが内部的に使用する IP アドレスの数	2
ノードで使用可能な使用可能な IP アドレスの合計	14 - 2 = 12
4 つのリモート リーフ スイッチに必要な IP アドレスの数	4 * 2 = 8
2 つの vPC ペアに必要な IP アドレスの数	2 * 1 =2
リモート プールで使用されている IP アドレスの合計	8 + 2 = 10
/28 リモート プールの空き IP アドレス	12 - 10 = 2

リモート リーフ スイッチを廃止すると、2 つの IP アドレスが解放されますが、24 時間が経過した後にのみ再利用できます。

GUI を使用してリモート リーフ スイッチのポッドとファブリック メンバーシップを設定する

IPN ルータとリモート スイッチを検出して接続するために、Cisco APIC を設定して有効にすることができます。ウィザードを使用するか、またはウィザードを使用せずに APIC GUI を使用する方法があります。

ダイレクト トラフィック フォワーディングについて

リリース4.1(2) でのリモート リーフ スイッチ動作の特性 （2 ページ）で説明されているように、直接トラフィック転送のサポートはリリース 4.1（2）以降でサポートされ、リリース 5.0（1）以降ではデフォルトで有効になっており、無効にすることはできません。ただし、直接トラフィック転送を有効または無効にするために使用する方法は、リモート リーフ スイッチで実行されているソフトウェアのバージョンによって異なります。

- リモート リーフ スイッチが現在リリース 4.1（2）以降で実行されている場合（リモート リーフ スイッチが 4.1（2）より前のリリースで実行されていない場合）、「ウィザードを使用してリモート リーフ スイッチのポッドとファブリック メンバーシップを構成する」手順に移動してください。
- リモート リーフ スイッチが現在 4.1（2）よりも前のリリースで稼働している場合は、「リモート リーフ スイッチのアップグレードおよび直接トラフィック転送の有効化」手順に移動してスイッチをリリース 4.1（2）以降にアップグレードし、必要な構成変更を行い、それらのリモート リーフ スイッチで直接トラフィック転送を有効にします。
- リモート リーフ スイッチがリリース 4.1(2) 以降で実行されており、ダイレクト トラフィック転送が有効になっているが、4.1（2）以前のリリースへ **ダウングレード** したい場合、「直接トラフィック転送を無効化、およびリモート リーフ スイッチのダウングレード」手順へ移動してこれらのリモート リーフ スイッチをダウングレードする前に直接トラフィック転送機能を無効化します。
- リモート リーフ スイッチがリリース 5.0（1）より前のリリースで実行されており、リリース 5.0（1）以降にアップグレードする場合：

  1. リモート リーフ スイッチが 4.1（2）より前のリリースで実行されている場合は、最初にリリース 4.1（2）にアップグレードし、「リモート リーフ スイッチのアップグレードおよび直接トラフィック転送の有効化」で説明されている手順を使用してそれらのリモート スイッチで直接トラフィック転送を有効にします。

2. リモート リーフ スイッチがリリース 4.1（2）にあり、ダイレクト トラフィック転送が有効になっている場合は、リモートリーフスイッチをリリース5.0（1）以降にアップグレードします。

- リモート リーフ スイッチがリリース 5.0（1）以降で実行されており、直接トラフィック転送がデフォルトで有効になっている場合、直接トラフィック転送もサポートしている次の以前のリリースにダウングレードする必要があります。
  - リリース 4.2（x）
  - リリース 4.1（2）

  直接トラフィック転送は、構成に応じてデフォルトで有効になっている場合とされていない場合があります：
  - ルーティング可能なサブネットとルーティング可能な Ucast の両方がダウングレード前にすべてのポッドで有効にされていた場合、ダウングレード後も直接トラフィック転送はデフォルトで有効のままになります。
  - ルーティング可能なサブネットがすべてのポッドで有効になっているが、ルーティング可能なUcastが有効になっていない場合、ダウングレード後、直接トラフィック転送は有効になりません。

リモート リーフ スイッチのフェールオーバー

（APIC）リリース 4.2（2）以降、 [Cisco Application Policy Infrastructure Controller] リモート リーフ スイッチはポッド冗長です。つまり、マルチポッドのセットアップでは、ポッド内のリモート リーフ スイッチがスパイン スイッチへの接続を失うと、別のポッドに移動されます。これにより、元のポッドに接続されているリモート リーフ スイッチのエンドポイント間のトラフィックが機能します。

リモート リーフ スイッチはポッドに関連付けられ、ピン接続され、スパイン プロキシ パスは設定によって決定されます。以前のリリースでは、Council of Oracle Protocol（COOP）はマッピング情報をスパイン プロキシに伝達していました。現在、スパイン スイッチへの通信が失敗すると、COOP セッションは別のスパイン スイッチのポッドに移動します。

以前は、Border Gateway Protocol（BGP）ルート リフレクタをポッドに追加しました。ここで、外部ルート リフレクタを使用し、ポッド内のリモート リーフ スイッチが他のポッドと BGP 関係を持っていることを確認します。

リモート リーフ スイッチのフェールオーバーは、デフォルトでは無効になっています。次にあるリモート リーフ ポッド [Cisco Application Policy Infrastructure Controller] 冗長性ポリシーを有効にします。 **[システム（Systems）]** > **[システム設定（System Settings）]** タブの（APIC）GUI内にあります。冗長プリエンプションを有効にすることもできます。プリエンプションを有効にすると、リモート ポッドがバックアップされると、リモート リーフ スイッチは親ポッドに再関連付けされます。プリエンプションを有効にしない場合、リモートリーフは、親ポッドが復帰しても動作ポッドに関連付けられたままになります。

（注） あるポッドから別のポッドにリモート リーフ スイッチを移動すると、数秒のトラフィックの中断が発生する可能性があります。

リモート リーフの復元力

リモート リーフ アーキテクチャの課題

現在のリモート リーフ アーキテクチャは、APIC、コントロール プレーン、およびデータ プレーンをメイン Pod のスパイン スイッチに直接結び付けます。

このアーキテクチャには、次の制約があります：

- リモート リーフ エンドポイント（EP）学習は、メイン Pod に関連付けられたコントロール プレーンに依存しています。
- リモート リーフ L3Out 外部プレフィックスは、メイン Pod に関連付けられた BGP 構成に依存します。
- メイン Pod スパインへの接続で障害が発生すると、リモート リーフ ノードのトラフィック転送に影響を与える可能性があります。

リモート リーフの復元力

リモート リーフの復元力は、複数のリモート リーフで構成されるグループを使用して実現されます。このグループが作成されると、リモート リーフ復元力グループ内のリモート リーフがフルメッシュの BGP EVPN セッションを形成して、エンドポイント情報と外部プレフィックス情報を交換します。WAN またはメイン Pod で障害が発生しても、リモート リーフ復元グループ内のトラフィックには影響しません。

リモートリーフの復元力を展開する場合、グループ内のリモートリーフは、シスコ独自のプロトコルではなく、BGP EVPN ベースの標準的なアプローチを使用して通信します。

このソリューションは、

- エンドポイントの学習を促進するために、リモートリーフの復元力グループ内にローカル BGP EVPN メッシュセッションを確立します。
- リモート リーフ復元力グループ内にフルメッシュ VPNv4 および VPNv6 セッションを確立して、L3Out 外部プレフィックスを配布します。
- データ転送のためにリモート リーフ復元力グループ内の BGP EVPN で学習したエンドポイントを使用します。
- リモートリーフ サイトとメイン Pod 間で COOP が学習したエンドポイントを利用します。

（注） リモート リーフ復元力グループへまたは、リモート リーフ復元力グループからの移行は、メンテナンス期間中に実行する必要があります。

リモート リーフ復元力グループの制限

リモート リーフ復元力グループには、次のような制限があります。

- 複数のリモート リーフ復元力グループでリモート リーフ TEP プールを構成することはできません。
- 異なる Pod からのリモート リーフ TEP プールを同じリモート リーフ復元力グループ内に構成することはできません。

GUI を使用してリモートリーフレジリエンシグループを作成する

GUIを使用してリモート リーフ レジリエンシ グループを作成するには、次の手順を実行します。

始める前に

ファブリック ACI サイトのすべてのスパインと ToR スイッチは、ファブリックでリモート リーフ レジリエンシ グループ機能を有効にする前に R6.1.3 にアップグレードする必要があります。

手順

ステップ 1 メニューバーで、**[ファブリック（Fabric）] > [インベントリ（Inventory）]**を選択します。

ステップ 2 ナビゲーション ペインで **[ポッド ファブリック設定ポリシー（Pod Fabric Setup Policy）]**を選択します。

[ポッド ファブリック設定ポリシー（Pod Fabric Setup Policy）] ペインが表示されます。

ステップ 3 ポッドをダブルクリックします。

[POD 向けファブリック セットアップ ポリシー（Fabric Setup Policy for a POD）] ペインが表示されます。

ステップ 4 **[自律 RL グループ（Autonomous RL Group）]** エリアに移動し、**[+]** 記号をクリックします。

[自律 RL グループの作成（Create Autonomous RL Group）] ダイアログボックスが表示されます。

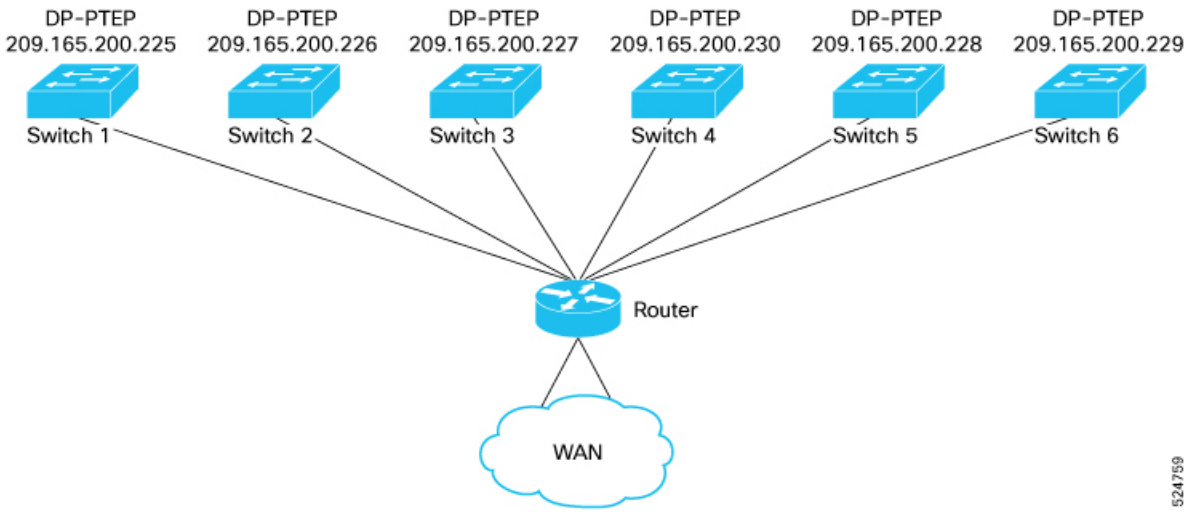
ステップ 5 グループ名フィールドにリモート リーフ レジリエンシ グループ名を入力します。

ステップ 6 **[+]** 記号をリモート ID フィールドに入力し、リモート リーフをこのグループにグループ化する TEP プールを選択します。

ステップ 7 リモート リーフ レジリエンシ グループを作成するために **[送信（Submit）]** をクリックします。

リモート リーフ レジリエンシ グループの詳細は、**[自律 RL グループ（Autonomous RL Group）]** エリアの **[ファブリック設定ポリシー（Fabric Setup Policy）]** ペインに表示されます。

CLIを使用してリモートリーフのレジリエンシの構成を確認します



6 つのスイッチすべてを 1 つのグループに構成します。

CLI を使用してリモート リーフのレジリエンシの構成を確認するには、次の手順に従います。

手順

ステップ 1 **show bgp l2vpn evpn summary vrf all** コマンドを実行して、すべてのリモート リーフ間のフルメッシュBGP L2VPN または EVPN セッションを表示します。

例：

```
Switch1# show bgp l2vpn evpn summary vrf all
BGP summary information for VRF overlay-1, address family L2VPN EVPN
BGP router identifier 105.1.1.1, local AS number 100
BGP table version is 254997, L2VPN EVPN config peers 5, capable peers 5
117325 network entries and 130831 paths using 22327320 bytes of memory
BGP attribute entries [2374/493792], BGP AS path entries [0/0]
BGP community entries [0/0], BGP clusterlist entries [1/4]

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
209.165.200.230      4   100  130445     291   254997    0    0 01:43:11 13908
209.165.200.226      4   100  149893     291   254997    0    0 01:43:11 8402
209.165.200.228      4   100     218     169   254997    0    0 01:43:02 1
```

```
209.165.200.229      4   100   69471     208   254997    0    0 01:30:49 30399
209.165.200.227      4   100    3505     291   254997    0    0 01:43:10 201
```

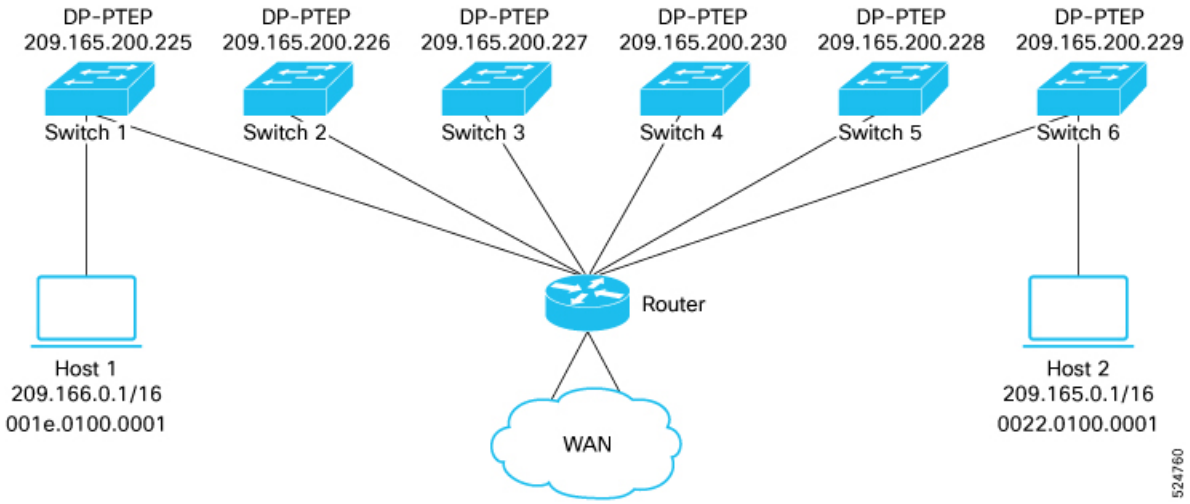
ステップ 2 **show bgp vpn unicast summary vrf overlay** コマンドを使用して、すべてのリモート リーフ間のフルメッシュ BGP VPN4 および VPN6 セッションを表示します。

例：

```
leaf5# show bgp vpnv4 unicast summary vrf overlay-1
BGP summary information for VRF overlay-1, address family VPNv4 Unicast
BGP router identifier 105.1.1.1, local AS number 100
BGP table version is 115527, VPNv4 Unicast config peers 7, capable peers 7
31202 network entries and 40403 paths using 5165136 bytes of memory
BGP attribute entries [1400/291200], BGP AS path entries [0/0]
BGP community entries [0/0], BGP clusterlist entries [1/4]

Neighbor           V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
11.1.1.165         4   100   57163     249   115527    0    0 01:45:33 400  >>>  This is session
with spine 1
11.1.1.240         4   100   57724     249   115527    0    0 01:45:34 400  >>> This is session with
 spine 2
209.165.200.230    4   100  130447     293   115527    0    0 01:45:37 2400
209.165.200.226    4   100  149895     293   115527    0    0 01:45:38 2400
209.165.200.228    4   100     220     171   115527    0    0 01:45:29 0
209.165.200.229    4   100   69723     210   115527    0    0 01:33:16 4400
209.165.200.227    4   100    3507     293   115527    0    0 01:45:37 0

leaf5# show bgp vpnv6 unicast summary vrf overlay-1
BGP summary information for VRF overlay-1, address family VPNv6 Unicast
BGP router identifier 105.1.1.1, local AS number 100
BGP table version is 101009, VPNv6 Unicast config peers 7, capable peers 7
26895 network entries and 31990 paths using 4779900 bytes of memory
BGP attribute entries [1200/249600], BGP AS path entries [0/0]
BGP community entries [0/0], BGP clusterlist entries [1/4]

Neighbor           V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
11.1.1.165         4   100   57164     250   101009    0    0 01:46:04 200
11.1.1.240         4   100   57725     250   101009    0    0 01:46:04 200
209.165.200.230    4   100  130448     294   101009    0    0 01:46:08 2400
209.165.200.226    4   100  149896     294   101009    0    0 01:46:08 2400
209.165.200.228    4   100     221     172   101009    0    0 01:45:59 0
209.165.200.229    4   100   69733     211   101009    0    0 01:33:46 2810
209.165.200.227    4   100    3508     294   101009    0    0 01:46:08 0
```

CLI を使用したエンドポイント間通信の確認

スイッチ 1 の場合、209.166.0.1（EPG-1）はローカルで学習された EP で、209.165.0.1（EPG-2）はリモート EP です。スイッチ 6 の場合、209.165.0.1 はローカルで学習された EP で、209.166.0.1 はリモート EP です。両方のエンドポイントは異なるサブネット内にあり、両方の EPG は switch1 と switch6 の両方で拡張されます。ローカル EP とリモート EP の Switch1 で取得される CLI出力をコンポーネントごとに示します。



CLI を使用して EP 間通信を確認するには、次の手順に従います。

手順

ステップ 1 **show system internal epm endpoint ip** コマンドを使用して、EPM の Switch1 のローカル EP エントリとリモート EP エントリを確認します。

例：

```
Switch1# show system internal epm endpoint ip 209.166.0.1
MAC : 001e.0100.0001 ::: Num IPs : 1
IP# 0 : 209.166.0.1 ::: IP# 0 flags :  ::: l3-sw-hit: No
Vlan id : 124 ::: Vlan vnid : 19003 ::: VRF name : ARL_Scale:ctx-1
BD vnid : 16023537 ::: VRF vnid : 2490424
Phy If : 0x1a014000 ::: Tunnel If : 0
Interface : Ethernet1/21
Flags : 0x80004c04 ::: sclass : 16388 ::: Ref count : 5
EP Create Timestamp : 02/05/2025 08:01:55.278575
EP Update Timestamp : 02/05/2025 09:21:27.898869
EP Flags : local|IP|MAC|sclass|timer|


Switch1# show system internal epm endpoint ip 209.165.0.1
MAC : 0000.0000.0000 ::: Num IPs : 1
IP# 0 : 209.165.0.1 ::: IP# 0 flags :  ::: l3-sw-hit: No
Vlan id : 0 ::: Vlan vnid : 0 ::: VRF name : ARL_Scale:ctx-1
BD vnid : 0 ::: VRF vnid : 2490424
Phy If : 0 ::: Tunnel If : 0x1801000b
Interface : Tunnel11
Flags : 0x80004410 ::: sclass : 16388 ::: Ref count : 3
EP Create Timestamp : 02/05/2025 08:17:38.279265
EP Update Timestamp : 02/05/2025 09:28:53.848534
EP Flags : locally-aged|IP|sclass|timer|
```

ステップ 2 **show interface tunnel** コマンドを実行します。

例：

```
Switch1# show interface tunnel 11
Tunnel11 is up
    MTU 9000 bytes, BW 0 Kbit
    Transport protocol is in VRF "overlay-1"
    Tunnel protocol/transport is ivxlan
    Tunnel source 209.165.200.225/32 (lo2)
    Tunnel destination 209.165.200.229

Tunnel is pointing to Switch6 dp-ptep IP.
```

ステップ 3 **show system internal tglean endpoint ip** コマンドを使用して、TgleanのSwitch1のローカル EP エントリとリモート EP エントリを確認します。

例：

```
Switch1# show system internal tglean endpoint ip 209.166.0.1

------------------------------------------------------------
             TGLEAN Oper Endpoint Information
------------------------------------------------------------

MAC : 001e.0100.0001 ::: Num IPs : 1
IP# 0 : 209.166.0.1
Vlan id : 123 ::: BD vnid : 16023537 ::: VRF vnid : 2490424
Sclass : 16388 ::: Interface : Ethernet1/21
EPM EP Flags : local|IP|MAC|
LRN SRC : EPM|
CFG Flags :
```

ネクスト ホップは、以下の出力のリモート EP 209.165.0.1 のスイッチ 6 の DP-PTEP IP を指します。

```
Switch1# show system internal tglean endpoint ip 209.165.0.1

------------------------------------------------------------
             TGLEAN Oper Endpoint Information
------------------------------------------------------------

MAC : 0000.0000.0000 ::: Num IPs : 1
IP# 0 : 209.165.0.1
Vlan id : 0 ::: BD vnid : 0 ::: VRF vnid : 2490424
Sclass : 16388 ::: EP NH : 209.165.200.229
EPM EP Flags : IP|
LRN SRC : EPM|UXRIB|
CFG Flags :
```

ステップ 4 **show l2route mac-ip all** コマンドを使用して、L2RIB の Switch1 のローカル EP エントリとリモート EP エントリを確認します。

例：

```
Switch1# show l2route mac-ip all | grep 209.166.0.1
123         001e.0100.0001 209.166.0.1  Local  PS,Orp        0     Eth1/21 (SGT - IP:16388)


Switch1# show l2route mac-ip all | grep 209.165.0.1
123         0022.0100.0001 209.165.0.1   BGP    --   0   209.165.200.229 (Label: 16023537) (SGT -
IP:16388)
```

ステップ 5 **show bgp l2vpn evpn vrf overlay** コマンドを使用して、他のピアに対する BGP のローカル EP アドバタイズメントを確認します。

例：

```
Switch1# show bgp l2vpn evpn 209.166.0.1 vrf overlay-1
Route Distinguisher: 105:16023537    (L2VNI 16023537)
BGP routing table entry for [2]:[0]:[0]:[48]:[001e.0100.0001]:[32]:[209.166.0.1]/272, version 59832
 dest ptr 0x8b0825e0
Paths: (1 available, best #1)
Flags: (0x0000000000000102 0000000000) on xmit-list, is not in rib/evpn
Multipath: eBGP iBGP

  Advertised path-id 1
  Path type (0x8b45d1a8): local 0x4000008c 0x4000000 ref 0 adv path ref 1, path is valid, is best
path, orphan host
  AS-Path: NONE, path locally originated
    0.0.0.0 (metric 0) from 0.0.0.0 (105.1.1.1)
     Origin IGP, MED not set, localpref 100, weight 32768 tag 0, propagate 0, floating svi 0, tunnel
 resolved 0
     Received label 16023537 2490424
     Extcommunity:
         RT:100:2490424
         RT:100:16023537
         PCTAG:00:0:0:16388

  Path-id 1 advertised to peers:
    209.165.200.230   209.165.200.226   209.165.200.229   209.165.200.227
```

ステップ 6　**show bgp l2vpn evpn vrf overlay** コマンドを使用して、BGP L2VPN EPVN セッションを通じて学習したリモート EP エントリを確認します。

例：

```
Switch1# show bgp l2vpn evpn 209.165.0.1 vrf overlay-1
Route Distinguisher: 105:16023537    (L2VNI 16023537)
BGP routing table entry for [2]:[0]:[0]:[48]:[0022.0100.0001]:[32]:[209.165.0.1]/272, version 211779
 dest ptr 0x192c7d44
Paths: (1 available, best #1)
Flags: (0x0000000000000212 0000000000) on xmit-list, is in rib/evpn, is not in HW
Multipath: eBGP iBGP

  Advertised path-id 1
  Path type (0x8998b550): internal 0xc0000018 0x400 ref 0 adv path ref 1, path is valid, is best
path, remote nh not installed, in rib
             Imported from (0x16757068)
108:16023537:[2]:[0]:[0]:[48]:[0022.0100.0001]:[32]:[209.165.0.1]/144
  AS-Path: NONE, path sourced internal to AS
    209.165.200.229 (metric 3) from 209.165.200.229 (108.1.1.1)
      Origin IGP, MED not set, localpref 100, weight 0 tag 0, propagate 0, floating svi 0, tunnel
resolved 0
      Received label 16023537 2490424
      Extcommunity:
          RT:100:2490424
          RT:100:16023537
          ENCAP:8
          PCTAG:00:0:0:16388
          Router MAC:000c.0c0c.0c0c

  Path-id 1 not advertised to any peer

Route Distinguisher: 108:16023537
BGP routing table entry for [2]:[0]:[0]:[48]:[0022.0100.0001]:[32]:[209.165.0.1]/272, version 210701
 dest ptr 0x899cc898
Paths: (1 available, best #1)
```

```
Flags: (0x0000000000000202 0000000000) on xmit-list, is not in rib/evpn, is not in HW, is locked
Multipath: eBGP iBGP

  Advertised path-id 1
  Path type (0x16757068): internal 0x40000018 0x4002000 ref 2 adv path ref 1, path is valid, is best
 path, remote nh not installed
              Imported to 2 destination(s)
  AS-Path: NONE, path sourced internal to AS
    209.165.200.229 (metric 3) from 209.165.200.229 (108.1.1.1)
      Origin IGP, MED not set, localpref 100, weight 0 tag 0, propagate 0, floating svi 0, tunnel
resolved 0
      Received label 16023537 2490424
      Extcommunity:
          RT:100:2490424
          RT:100:16023537
          ENCAP:8
          PCTAG:00:0:0:16388
          Router MAC:000c.0c0c.0c0c

  Path-id 1 not advertised to any peer
```

ステップ 7 **show ip route** コマンドを使用して、URIB の /32 ルートとしてリモート EP エントリを確認します。ローカル EP の場合、URIB に /32 ルートとしてのエントリはありません。

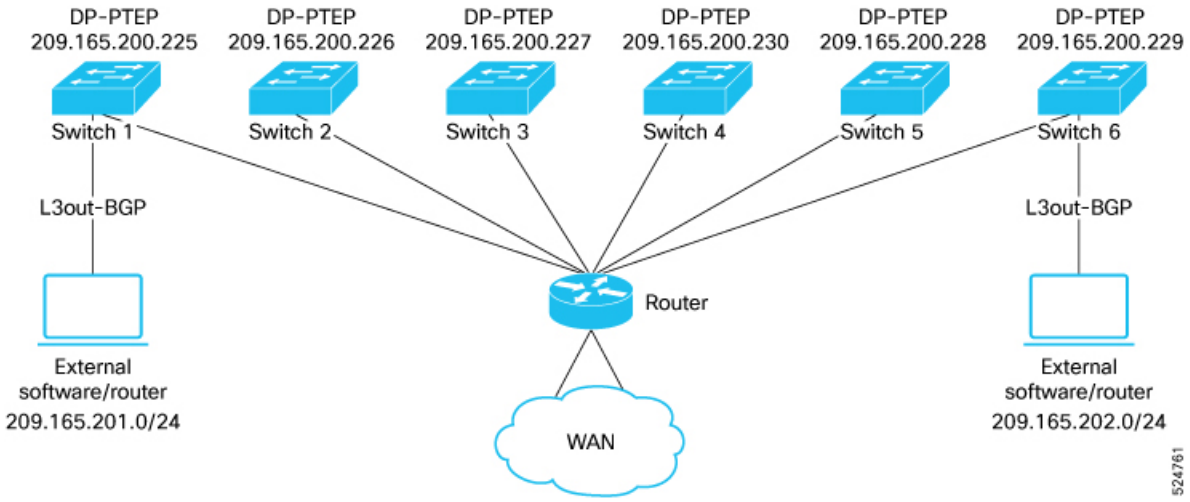
例：

```
Switch1# show ip route 209.165.0.1/32 vrf ARL_Scale:ctx-1
IP Route Table for VRF "ARL_Scale:ctx-1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

209.165.0.1/32, ubest/mbest: 1/0, pervasive
    *via 209.165.200.229%overlay-1, [200/0], 01:37:08, bgp-100, internal, tag 100, redist-only,
rwVnid: vxlan-2490424, pc-tag: 16388
         recursive next hop: 209.165.200.229/32%overlay-1

Next hop is pointing to Switch6 dp-ptep IP.
```

ユーザーが switch6 の EPG-1 と switch1 の EPG-2 を拡張しない場合、すべてのCLI出力は上記と同じになりますが、リモート EP の L2RIB エントリは両方のスイッチで表示されません。

CLIを使用した L3OUT から L3OUT への通信の確認

Switch1 は 209.165.201.0/24 を L3OUT 経由でローカルに学習し、Switch6 は 209.165.202.0/24 を L3OUT 経由でローカルに学習する。Switch1 は、Switch6 の DP-PTEP IPアドレス（209.165.200.229）としてネクストホップとの VPNV4 BGP ピアリングを介して 209.165.202.0/24 を受信します。同様に、Switch6 は、Switch1 の DP-PTEP IPアドレス（209.165.200.225）としてのネクスト ホップとの VPNV4 BGP ピアリングを介して 209.165.201.0/24 を受信します。



CLI を使用して L3OUT から L3OUT への通信を確認するには、次の手順を実行します。

手順

ステップ 1 次のスーパーユーザー権限で、 **show bgp vpnv4 unicast vrf overlay** コマンドを使用します。

例：

```
Switch1# show bgp vpnv4 unicast 209.165.202.0/24 vrf overlay-1
BGP routing table information for VRF overlay-1, address family VPNv4 Unicast
Route Distinguisher: 105:2490424    (VRF ARL_Scale:ctx-1)
BGP routing table entry for 209.165.202.0/24, version 1946 dest ptr 0x8b3963b8
Paths: (1 available, best #1)
Flags: (0x00000000000c001a 0000000000) on xmit-list, is in urib, is best urib route, is in HW,
exported
  vpn: version 145728, (0x0000000000100002) on xmit-list
Multipath: eBGP iBGP

  Advertised path-id 1, VPN AF advertised path-id 1
  Path type (0x173c502c): internal 0xc0000018 0x440 ref 0 adv path ref 2, path is valid, is best
path, in rib
             Imported from (0x164de938) 108:2490424:209.165.202.0/24
  AS-Path: 65001 , path sourced external to AS
    209.165.200.229 (metric 3) from 209.165.200.229 (108.1.1.1)
      Origin IGP, MED not set, localpref 100, weight 0 tag 0, propagate 0, floating svi 0, tunnel
resolved 0
      Received label 0
      Received path-id 1
      Extcommunity:
          RT:100:2490424
          VNID:2490424

  VRF advertise information:
  Path-id 1 advertised to peers:
    21.2.1.1           21.2.1.10

  VPN AF advertise information:
  Path-id 1 not advertised to any peer
```

```
BGP routing table information for VRF overlay-1, address family VPNv4 Unicast
Route Distinguisher: 108:2490424
BGP routing table entry for 209.165.202.0/24, version 144468 dest ptr 0x173596e8
Paths: (1 available, best #1)
Flags: (0x0000000000000002 0000000000) on xmit-list, is not in urib, is not in HW, is locked
Multipath: eBGP iBGP

  Advertised path-id 1
  Path type (0x164de938): internal 0x40000018 0x40 ref 1 adv path ref 1, path is valid, is best path

             Imported to 1 destination(s)
  AS-Path: 65001 , path sourced external to AS
    209.165.200.229 (metric 3) from 209.165.200.229 (108.1.1.1)
      Origin IGP, MED not set, localpref 100, weight 0 tag 0, propagate 0, floating svi 0, tunnel
resolved 0
      Received label 0
      Received path-id 1
      Extcommunity:
          RT:100:2490424
          VNID:2490424

  Path-id 1 not advertised to any peer
```

ステップ 2 次のスーパーユーザー権限で、 **show ip route** コマンドを使用します。

例：

```
Switch1# show ip route 209.165.202.13 vrf ARL_Scale:ctx-1
IP Route Table for VRF "ARL_Scale:ctx-1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

209.165.202.0/24, ubest/mbest: 1/0
    *via 209.165.200.229%overlay-1, [200/0], 00:23:41, bgp-100, internal, tag 65001
         recursive next hop: 209.165.200.229/32%overlay-1
```

リモートのリーフスイッチのダウングレードする前に必要な前提条件

（注） リモート ノードの使用停止し、リモート リーフに関連するポリシー（を削除する必要がありますがあれば導入で、リモートのリーフ スイッチ リリース 3.1（1）から以降、リモート リーフ機能をサポートしていない以前のリリースには、APIC ソフトウェアのダウン グレードする場合、というプールにある）を含む前にダウングレードします。スイッチの廃止の詳細については、スイッチのデコミッションおよび再コミッションを参照してください。これは、「*Cisco APIC* トラブルシューティング ガイド」にあります。

リモート リーフ スイッチをダウン グレードする前に、いずれかのタスクが完了することを確認します。

- vPC ドメインを削除します。
- SCVMM を使用している場合は、vTEP - 仮想ネットワーク アダプタを削除します。
- リモート リーフ ノードの使用停止および10を待機-15分を完了するタスクの使用停止後。
- 削除に WAN L3out にリモート リーフ、テナント インフラ。
- Multipod を使用している場合、インフラ-l3out VLAN 5 とを削除します。
- リモートというプールを削除します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。